Customer No. 24498 **PATENT**
Attorney Docket No. PF030028
Office Action dated: February 26, 2010

REMARKS

The Office Action mailed February 26, 2010 has been reviewed and carefully considered. No new matter has been added.

Claim 27 has been amended. Claims 1-7, 9-13, 15-19, 21-24, and 26-27 are pending.

Claims 1-7, 9-13, 15-18, 21, and 25 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,904,522 to Benardeau et al. (hereinafter "Benardeau") in view of U.S. Patent Publication No. 2002/0170053 to Peterka et al. (hereinafter "Peterka") in further view of U.S. Patent Publication No. 2006/0200417 to Stefik et al. (hereinafter "Stefik"). Claims 19, 22, 26, and 27 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Benardeau in view of U.S. Patent Application Publication No. 2006/0212399 to Akiyama (hereinafter "Akiyama"). Claims 23 and 24 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Benardeau in view of Peterka in further view of Stefik in view of Akiyama in further view of U.S. Patent No. 7,302,571 to Noble et al. (hereinafter "Noble"). The rejections are respectfully traversed.

The independent claims in the instant application are Claims 1, 13, 19, 22, and 27.

It is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest the following limitations of Claim 1:

> a master digital terminal and at least one slave digital terminal adapted to generally simultaneously receive protected digital data from a transmitter, the at least one slave digital terminal being connected to the master terminal by a link,
>
> wherein said at least one slave digital terminal is adapted to receive a message from the transmitter instructing said at least one slave digital terminal to delete stored information necessary for accessing said protected digital data, to request, after receiving the message, from the master digital terminal new information necessary for accessing said protected digital data, and await the new information until an expiration of a predetermined deadline counted from a transmission of the request.

Further, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest the following limitations of Claim 13:

> A digital terminal intended to receive protected digital data from a transmitter generally simultaneously with a second digital terminal, wherein the digital terminal is adapted to receive a message from the transmitter instructing the digital terminal to delete stored information necessary for accessing said data and received by the second digital terminal to which it can be connected, to request, after receiving the message, from the second digital terminal new information necessary for accessing said protected digital data, and await the new information until an expiration of a predetermined deadline counted from a transmission of the request.

Initially, we point out that it appears that Benardeau and Peterka may not be combined, in the manner suggested since the arrangement of the two references are entirely different in their operation Benardeau teaches a master-slave couple that is paired and which requires the slave to request information from the master, whereas Peterka teaches a system in which either **each** client requests new keys or a server sends the keys to the clients. It would seem quite difficult, if even possible in the first place, to combine a system in which a slave device is clearly dependent on the master and a system in which each client acts independently. Also, why would the skilled person combine the paired solution of Benardeau with the non-paired solution of Peterka when it would seem so much easier to entirely one mode and simply use Peterka without Benardeau. The answer would appear to be impermissibly hindsight construction with the present claims in mind, in contravention of, for example, MPEP §2141.01(III).

Further, such a combination would contravene MPEP §2143.01, which explicitly prohibits the combining of two or more references where such resultant combination changes the principle of operation of the prior art invention being modified. The following text of MPEP §2143.01 is provided in pertinent part:

> If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959) (Claims were directed to an oil seal comprising a bore engaging portion with outwardly biased resilient spring fingers inserted in a resilient sealing member. The primary

reference relied upon in a rejection based on a combination of references disclosed an oil seal wherein the bore engaging portion was reinforced by a cylindrical sheet metal casing. Patentee taught the device required rigidity for operation, whereas the claimed invention required resiliency. The court reversed the rejection holding the "suggested combination of references would require a substantial reconstruction and redesign of the elements shown in [the primary reference] as well as a change in the basic principle under which the [primary reference] construction was designed to operate." 270 F.2d at 813, 123 USPQ at 352.).

Here, as noted above, Benardeau discloses a system in which a slave device is clearly dependent on the master while Peterka discloses a system in which each client acts independently. Given the preceding disparate principles of operation, any modification of Benardeau with the teachings of Peterka or vice versa would respectively change the principle of operation of Benardeau or Peterka, in contravention to MPEP §2143.01.

Hence, any combination of references under 35 U.S.C. 103 involving both Benardeau and Peterka is improper and should be withdrawn in consideration of at least MPEP §2143.01, as well as in consideration of the prohibition against impermissible hindsight (see, e.g., MPEP §2141.01(III)).

In any event, we submit that even if combined, the references still fail to disclose each and every limitation of the claims. Cited paragraph [0107] of Peterka discloses that in a pull model, "each client keeps track of the keys and their expiration times and actively requests new keys before the current keys expire so as to avoid service interruptions". Moreover, cited paragraph [0107] of Peterka further discloses that the "push model migrates the responsibility to the server which keeps track of active clients and distributes new keys to them before the current keys expire".

However, the Examiner argues that Peterka, using the push model, sends messages with new keys to delete the old key (see, e.g., pending Office Action dated February 26, 2010, p. 4, lines 7-10). We respectfully disagree with the Examiner's reading of Peterka. For example, the entire disclosure of Peterka is completely silent regarding the feature of instructing the clients to **delete** the information. Rather, it seems that the server sends a message without any

requirements as to the old keys. It is thus abundantly clear that Peterka does not teach the feature of "adapted to receive a message from the transmitter instructing said at least one slave digital terminal to delete stored information necessary for accessing said protected digital data" as recited in Claim 1. The Applicants cannot find any mention of the "reminder messages" mentioned by the Examiner, for example, at page 4, lines 11-15 of the pending Office Action dated February 26, 2010.

Moreover, Claim 1 also requires the slave to request, after having received this message, new information from the master. First, in Peterka, the clients communicate with the server and there is no mention of passing a key to the slave device via a "master" device. Second, in the push model, the server sends the new keys to the client, as admitted by the Examiner himself, and there is no reason given as to why the client would then request data that it already has? While Benardeau arguably teaches the client sending messages to the master for decryption, we note that not having the information is not the same thing as having but not being able to decrypt the information

Hence, Benardeau fails to teach all the limitations in the second part of Claim 1, i.e. from "wherein said" until the end of the claim and the Examiner even admits the same on at least page 4 of the pending Office Action dated February 26, 2010.

Hence, Peterka fails to teach at least the following features of Claim 1:

- "wherein said at least one slave digital terminal is adapted to receive a message from the transmitter instructing said at least one slave digital terminal to delete stored information necessary for accessing said protected digital data". As already mentioned, Peterka fails to mention any "deletion instruction", as providing new keys for a following cryptoperiod is **not** the same.
- "to request, after receiving the message, from the master digital terminal new information necessary for accessing said protected digital data". Once again, we have shown above how it is pointless for the slave to request the keys it already has. In Peterka, the clients have the ability to decrypt the received keys, so there is no need to request further information or help to decrypt the keys.
- "await the new information until an expiration of a predetermined deadline counted from a transmission of the request." This is explicitly admitted by the Examiner on page 4 of the pending Office Action.

Moreover, we respectfully disagree with the Examiner's analysis of Benardeau when it comes to the "predetermined deadline". The Examiner argues that the predetermined deadline is the validity period of Kex and/or CW. However, if one looks at FIG. 6 of Benardeau, it is apparent that the slave 52 is not at all concerned with the validity period of Kex, but simply relies on the master 30 to use this key to decrypt the ECM and extract the CW. In addition, the slave does not exactly know the validity period of the CW. The slave may have an idea, but it is not sure and there is no mention of the slave waiting for a certain period of time.

The Examiner also mentions the validity period of Ks that is used to protect the master-slave link. For Ks, the Examiner cites column 14, lines 16-24 of Benardeau which disclose that a "new session key value may be generated at every subsequent reconnection of the decoder 50 and card 52 in the system, i.e. every time the decoder is switched on by a user, or at every viewing session, for example, of a pay per view film". These conditions are completely aleatory for the slave, which has no means of knowing when they occur. Also, when they do occur, a new Ks is generated and used. Hence it does not make any sense to argue that the slave waits a predetermined time since the time is not predetermined. In addition, there is no mention at all of the slave **waiting** a certain time; the skilled person will appreciate that the slave instead simply uses the current Ks.

Finally, the Examiner turns to Stefik to show the feature of "await the new information until an expiration of a predetermined deadline counted from a transmission of the request" as recited in Claim 1. According to the Examiner, this is taught in paragraph [0227] of Stefik, which describes verification as a time difference that is not too large.

First, the cited combination seems improper since the combination of Benardeau-Peterka, both deal with **broadcasts**, while Stefik does not. While all three are related to content distribution, their respective solutions are quite different. Hence, in view of the preceding, the argument set forth above regarding MPEP §2143.01 and any combination involving Benardeau and Peterka also applies in consideration of Stefik, as a combination of any two of Benardeau, Peterka, and Stefik results in a change in operation of the prior art invention being modified, in contravention to MPEP §2143.01.

Second, if one reads Stefik carefully, it becomes clear that [0227] is directed to the **synchronization of internal clocks**. The synchronization of internal clocks is achieved in Stefik as follows. Repository 2 of Stefik sends 1706 a timestamp message to repository 1 that then

generates 1707 and sends 1708 its timestamp message to repository 2. Upon reception of the message, repository 2 notes the current time 1709, saves the time 1710 received from repository 1 and compares 1711 the two times.

In other words, repository 2 receives a message with a time, then notes the current time and compares the noted current time and the received time. This achieves a verification that the clock of repository 1 is not too different from that of repository 2. For instance, repository 1 waits 15 years before returning its timestamp. Upon reception of the message (transmitted, we assume, with negligible delay), repository 1 will note the current time and compare the two times. Ideally, they match to within a few milliseconds. It is, in other words, abundantly clear that repository 2 does not wait a predetermined time for repository 1 to respond.

Hence, Stefik fails to teach the feature of "await the new information until an expiration of a predetermined deadline counted from a transmission of the request".

Thus, the combination of Benardeau, Peterka and Stefik (which is an improper combination for at least the reasons set forth above) does not teach more features than Benardeau by itself, and this is, as the Examiner kindly admits, far from all of the features of Claim 1.

Accordingly, it follows that Claim 1 is allowable over the cited references, either taken alone or in any combination with the cited references.

As Claim 13 comprises the "slave" decoder features as well as the "predetermined deadline" feature of claim 1, Claim 13 is allowable for essentially the same reasons as set forth above with respect to Claim 1.

Additionally, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest the following limitations of Claim 19:

> System for receiving broadcast digital data, comprising:
>
> a master digital terminal and at least one slave digital terminal adapted to generally simultaneously receive protected data from a transmitter, the at least one slave digital terminal being connected to the master terminal by a link,
>
> wherein said slave digital terminal can access said received protected digital data only if information necessary for accessing said protected digital data and received by the master digital terminal is sent by way of said link to the slave digital terminal within a predetermined deadline,

wherein the information necessary for accessing said protected digital data comprises filter parameters for extracting from the data stream received by the slave digital terminal a message containing access entitlements to the services for the slave digital terminal, and

wherein the at least one slave digital terminal comprises filters that use the filter parameters to extract the message containing the access entitlements.

Similar to Claims 1 and 13 argued above, and now argued with respect to Claim 19, Benardeau does not teach or suggest the feature of Claim 19 relating to at least the recited "predetermined deadline".

Moreover, Benardeau also fails to teach or suggest "wherein the at least one slave digital terminal comprises filters that use the filter parameters to extract the message containing the access entitlements", as recited in Claim 19. For example, Benardeau teaches a system in which an ECM is sent from the slave to the master, which decrypts the ECM to extract the CW, re-encrypts the CW with a session key Ks, and sends the re-encrypted CW to the slave where it is decrypted and used to descramble received broadcasts. It is also mentioned in Benardeau that the CWs may comprise copyright notification information that may be used to prevent the slave from performing certain actions, such as recording or playing back the data. However, the Examiner's arguments appear to not have any bearing on the recited limitations of Claim 19.

It would appear that there are no filter parameters in Benardeau. Certainly not any that enable the extraction of access entitlements. In Benardeau, the access entitlements, i.e., the CWs, are transmitted in the ECMs that are passed to the master, decrypted, re-encrypted, decrypted by the slave and used to descramble the content data. In other words, all the slave's access entitlements are **inside** the received message with the re-encrypted CWs. Once this has been decrypted, there are no more access entitlements to extract from the data stream.

It should also be noted that filtering and decryption are two completely different processes. Normally, filtering is used to decide what is to be decrypted.

In addition, according to Figure 5 of Benardeau, it is the slave that generates Ks and sends it to the master. Hence, the necessary information is not received from the master.

We also respectfully disagree with the Examiner's contention that anything else not encrypted with the Ks cannot be opened. This is not true, as Ks only decrypts the re-encrypted

CW. Otherwise, this would mean that the slave at this time cannot descramble the digital content; the slave receives the CW before it is needed. Hence, Benardeau's slave can always access everything for which it has access rights, but it cannot access anything else.

Thus, Benardeau also does not teach or suggest the "predetermined deadline" or the fourth feature reproduced above from Claim 19, namely "wherein the at least one slave digital terminal comprises filters that use the filter parameters to extract the message containing the access entitlements".

Applicants submit that it is irrelevant whether or not Akiyama teaches a filter for filtering access control messages. No matter how one interprets these references, there is simply no mention or hint at a combination that lets the slave receive the filter parameters from the master, and that those parameters enable extraction of the access entitlements by the slave.

Hence, it is believed that Claim 19 is allowable over the cited combination for at least the preceding reasons.

Moreover, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest the following limitations of Claim 22:

> A digital terminal intended to receive protected digital data from a transmitter generally simultaneously with a second digital terminal, wherein the digital terminal can access said received protected digital data only if information necessary for accessing said data and received by the second digital terminal to which it can be connected, is not received from this other terminal within a predetermined deadline,
>
> wherein the information necessary for accessing said protected digital data comprises filter parameters for extracting from the data stream received by the slave digital terminal a message containing access entitlements to the services for the slave digital terminal, and
>
> wherein the slave digital terminal comprises filters that use the filter parameters to extract the message containing the access entitlements.

Given the common limitations between Claims 19 and 22 reproduced above, it is respectfully asserted that Claim 22 is patentably distinct and non-obvious over the cited

references for at least the same reasons set forth above with respect to Claim 19. For example, at the least, the cited references fail to show the claimed feature relating to the "predetermined deadline" recited in Claim 22 and argued above as well as the following feature recited in Claim 22 and also essentially argued above "wherein the slave digital terminal comprises filters that use the filter parameters to extract the message containing the access entitlements".

Further, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest the following limitations of Claim 27:

> System for receiving broadcast digital data comprising:
>
> a master digital terminal and at least one slave digital terminal adapted to generally simultaneously receive protected digital data from a transmitter, the at least one slave digital terminal being connected to the master terminal by a link,
>
> wherein said slave digital terminal is adapted to receive from the transmitter a first part of an Entitlement Management message necessary for accessing said protected digital data, to receive from the master terminal a second part of the Entitlement Management Message necessary for accessing said protected digital data provided that it is received from the master digital terminal within a predetermined deadline, wherein the first part and the second part of the Entitlement Management Message enable accessing at least one decryption key for the protected digital data.

As noted above, Claim 27 has been amended. Support for the amendments to Claim 27 may be found at least in Figure 5 and the text corresponding thereto of the instant application.

Given the common limitations between Claim 27 and, for example, Claims 1, 13, 19, and 22 reproduced above, it is respectfully asserted that Claim 27 is patentably distinct and non-obvious over the cited references for at least the same reasons set forth above with respect to these claims. For example, at the least, the cited references fail to show the claimed feature relating to the "predetermined deadline" recited in Claim 27 and argued above, for example, where we mention that it is the slave that sends Ks to the master in Figure 6 of Benardeau.

Additionally, Benardeau fails to teach the transfer of EMM information from master to slave and there is also no mention in Benardeau of the slave receiving the EMM in two parts, one from the transmitter and the other from the master as now recited in amended Claim 27.

This feature is clearly absent also from Akiyama, which is silent regarding the same.

Hence, none of the cited references, either taken singly or in any combination, teach or suggest all of the above reproduced limitations of independent Claims 1, 13, 19, 22, and 27.

The failure of an asserted combination to teach or suggest each and every feature of a claim remains fatal to an obviousness rejection under 35 U.S.C. § 103. Section 2143.03 of the MPEP requires the "consideration" of every claim feature in an obviousness determination. To render a claim unpatentable, however, the Office must do more than merely "consider" each and every feature for this claim. Instead, the asserted combination of the patents must also teach or suggest *each and every claim feature*. *See In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974) (emphasis added) (to establish *prima facie* obviousness of a claimed invention, all the claim features must be taught or suggested by the prior art). Indeed, as the Board of Patent Appeal and Interferences has recently confirmed, a proper obviousness determination requires that an Examiner make "a searching comparison of the claimed invention - *including all its limitations* - with the teaching of the prior art." *See In re Wada and Murphy*, Appeal 2007-3733, *citing In re Ochiai*, 71 F.3d 1565, 1572 (Fed. Cir. 1995) (emphasis in original). "If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious" (MPEP §2143.03, citing *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)).

Accordingly, Claims 1, 13, 19, 22, and 27 are patentably distinct and non-obvious over the cited references for at least the reasons set forth above.

Claims 2-7, 9-12, 15, 17, 21, and 23-24 depend from Claim 1 or a claim which itself is dependent from Claim 1 and, thus, includes all the elements of Claim 1. Claims 16 and 18 depend from Claim 13 or a claim which itself is dependent from Claim 13 and, thus, includes all the elements of Claim 13. Claim 26 depends from Claim 19 and, thus, includes all the elements of Claim 19. Accordingly, Claims 2-7, 9-12, 15, 17, 21, and 23-24 are patentably distinct and non-obvious over the cited references for at least the reasons set forth above with respect to Claim 1, Claims 16 and 18 are patentably distinct and non-obvious over the cited references for at least the

reasons set forth above with respect to Claim 13, and Claim 26 is patentably distinct and non-obvious over the cited references for at least the reasons set forth above with respect to Claim 19.

Thus, reconsideration of the rejection is respectfully requested.

In view of the foregoing, Applicants respectfully request that the rejection of the claims set forth in the Office Action of February 26, 2010 be withdrawn, that pending claims 1-7, 9-13, 15-19, 21-24, and 26-27 be allowed, and that the case proceed to early issuance of Letters Patent in due course.

No fee is believed due with regard to the filing of this amendment. However, if a fee is due, please charge Deposit Account No. 07-0832.

Respectfully submitted,

Philippe Leyendecker, et al.

By: _____

Paul P. Kiel, Attorney for
Applicants
Registration No. 40,677
(609) 734-6815

Patent Operations
Thomson Licensing LLC
P.O. Box 5312
Princeton, NJ 08543-5312

Date: 4/29/10